	Application No.	Applicant(s)
Notice of Allowability	10/796,358	CONOVER, MATTHEW
	Examiner	Art Unit
	Marwan Ayash	2185

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed 8/24/07 & subsequent emailed amendment 9/13/07 after telephone interview.*

2. ☐ The allowed claim(s) is/are *1-5, 7-8, 11-15, 17-20, 25 (renumbered 1-17)* .

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20070913* .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

Response to Amendment

At this point, claims 1-5, 7-8, 11-15, 17-20, 25 have been amended. There are 17 claims pending in the

application, all of which are ready for reconsideration by the examiner.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be

unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of.

such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Serge Hodgson

(Reg. No. 40,017) on 9/13/07. The application has been amended as follows:

1. (Currently amended) A method comprising:

stalling a heap allocation function call to a heap allocation function originating from a request by an

application for a block of heap buffer;

predicting a predicted block of said heap buffer to fulfill said request, said predicted block comprising a

header portion and a data portion reserved for data; and

determining if a forward link (F-link) in a F-link field and a backward link (B-link) in a B-link field of

said header portion of said predicted block are addresses within a heap segment associated with said predicted

block, wherein upon a determination that said F-link and said B-link of said predicted block are not addresses

within said heap segment, said method further comprising taking corrective action comprising setting said F-link

and said B-link to be an address of a list head of a freelist comprising said predicted block.

2. (Original) The method of Claim 1 further comprising hooking said heap allocation function.

3. (Original) The method of Claim 1 further comprising determining a size of said block.

4. (Original) The method of Claim 3 wherein said predicted block has said size.

5. (Currently amended) The method of Claim 3 wherein a said freelist comprises a plurality of free blocks

having said size, said predicted block being on said freelist.

6. (Canceled)

7. (Currently amended) The method of Claim 6-1 further comprising determining whether a F-link of a predicted said list head of said predicted freelist points into said heap segment.

8. (Currently amended) The method of Claim 6-1 further comprising determining whether a B-link of a predicted next block of said predicted freelist points into said heap segment.

9-10 (Canceled)

11. (Currently amended) A method comprising:

stalling a heap deallocation function call to a heap deallocation function originating from a release by an application of a block of heap buffer, wherein said block is a deallocation block that is being deallocated to a deallocation freelist; and

determining if a forward link (F-link) in a F-link field of a header portion of a list head of said deallocation freelist and a backward link (B-link) in a B-link field of a header portion of a first block of said deallocation freelist are addresses within a heap segment associated with said deallocation freelist, said first block further comprising a data portion reserved for data, wherein upon a determination that said F-link is not an address within said heap segment, said method further comprising taking corrective action comprising setting said F-link and a B-link in a B-link field of a header portion of said list head to be an address of said list head.

12. (Currently amended) The method of Claim 11 further comprising reading said F-link and said B-link in said B-link field of said header portion of said first block.

13. (Original) The method of Claim 11 further comprising hooking said heap deallocation function.

14. (Previously presented) The method of Claim 11 further comprising determining said block being released by said application.

15. (Currently amended) The method of Claim 11 wherein upon a determination that said F-link and said B-link in said B-link field of said header portion of said first block are addresses within said heap segment, said method further comprising releasing said heap deallocation function call.

16. (Canceled)

17. (Currently amended) The method of Claim 11 wherein said F-link or said B-link in said B-link field of said header portion of said first block is a stray F-link or stray B-link, said method further comprising determining if said stray F-link or stray B-link is a known false positive.

18. (Original) The method of Claim 11 further comprising determining if said block is to be coalesced with other free blocks.

19. (Original) The method of Claim 11 wherein said block is to be coalesced with a coalesced block, said method further comprising:

        determining if a F-link and a B-link of said coalesced block are addresses within a heap segment associated with said coalesced block.

20. (Original) The method of Claim 19 further comprising determining if there are other blocks to be coalesced with said block.

21-24. (Canceled)

25. (Currently amended) A computer-program product comprising a tangible computer-readable storage medium containing computer program code comprising:

        a heap buffer overflow exploitation prevention application for stalling a heap allocation function call to a heap allocation function originating from a request by an application for a block of heap buffer;

        said heap buffer overflow exploitation prevention application further for predicting a predicted block of said heap buffer to fulfill said request, said predicted block comprising a header portion and a data portion reserved for data; and

        said heap buffer overflow exploitation prevention application further for determining if a forward link (F-link) in a F-link field and a backward link (B-link) in a B-link field of said header portion of said predicted block are addresses within a heap segment associated with said predicted block, wherein upon a determination that said F-link and said B-link of said predicted block are not addresses within said heap segment, said heap buffer overflow exploitation prevention application further for taking corrective action comprising setting said F-link and said B-link to be an address of a list head of a freelist comprising said predicted block.

Allowable Subject Matter

1.   Claims 1-5, 7-8, 11-15, 17-20, 25 are allowed.

2.   The following is an examiner's statement of reasons for allowance:

Claims 1, 25 are directed to means for preventing heap buffer overflow exploitation. These claims contain

allowable subject matter over the cited prior art because the cited prior art does not teach or suggest **the**

combination of all limitations as in the instant claim including: stalling a heap allocation function call to a

heap allocation function originating from a request by an application for a block of heap buffer; predicting a

predicted block of said heap buffer to fulfill said request, said predicted block comprising a header portion and a

data portion reserved for data; and determining if a forward link (F-link) in a F-link field and a backward link

(B-link) in a B-link field of said header portion of said predicted block are addresses within a heap segment

associated with said predicted block, wherein upon a determination that said F-link and said B-link of said

predicted block are not addresses within said heap segment, said method further comprising taking corrective

action comprising setting said F-link and said B-link to be an address of a list head of a freelist comprising said

predicted block.

        Claim 11 is directed to a method for preventing heap buffer overflow exploitation. This claim contains

allowable subject matter over the cited prior art because the cited prior art does not teach or suggest **the**

combination of all limitations as in the instant claim including: stalling a heap deallocation function call to a

heap deallocation function originating from a release by an application of a block of heap buffer, wherein said

block is a deallocation block that is being deallocated to a deallocation freelist; and determining if a forward link

(F-link) in a F-link field of a header portion of a list head of said deallocation freelist and a backward link (B-

link) in a B-link field of a header portion of a first block of said deallocation freelist are addresses within a heap

segment associated with said deallocation freelist, said first block further comprising a data portion reserved for

data, wherein upon a determination that said F-link is not an address within said heap segment, said method

further comprising taking corrective action comprising setting said F-link and a B-link in a B-link field of a

header portion of said list head to be an address of said list head.

Claims 2-5, 7-8, 12-15, 17-20, are allowable for at least the reason indicated with respect to claims 1, 11 above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."
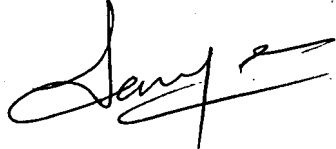
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Marwan Ayash whose telephone number is 571-270-1179. The examiner can normally be reached on Mon-Fri 10am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sanjiv Shah can be reached on (571)272-4098. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Marwan Ayash - Examiner - Art Unit 2185

9/13/07

SANJIV SHAH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100